Vysoká škola báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Absolvování individuální odborné praxe

Individual Professional Practice in the Company

204/2015 **Jan Schovánek**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání bakalářské práce

Student: **Jan Schovánek**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: Výzkumný ústav vodohospodářský T. G.Masaryka, v.v.i.
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
c. Zvolený postup řešení zadaných úkolů
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Podle pokynů konzultanta, který vedl odbornou praxi studenta

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Radim Kabeláč

Datum zadání: 01.09.2014

Datum odevzdání: 07.05.2015

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * OSTRAVA *

doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *5. května 2015*

Jan Schovánek

.....

podpis studenta

Poděkování

Rád bych poděkoval mému konzultantovi Radimu Kabeláčovi za možnost vykonání odborné praxe ve Výzkumném ústavu vodohospodářském T. G. Masaryka, v.v.i., a za odbornou pomoc a konzultaci při vytváření této bakalářské práce.

Rovněž bych rád poděkoval mé vedoucí Ing. Zdeňce Chmelíkové za pomoc a cenné rady při zpracování této bakalářské práce.

Prohlášení zástupce spolupracující právnické nebo fyzické osoby

„Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských/magisterských programech VŠB-TU Ostrava."

Dne: *5. května 2015*

.....
podpis zástupce

Abstrakt

Tato bakalářská práce popisuje průběh absolvování individuální odborné praxe ve Výzkumném ústavu vodohospodářském T. G. Masaryka v.v.i. V této práci popisuji analýzu současného stavu počítačové sítě a poté návrh nové počítačové sítě s ohledem na usnadnění správy. Poslední kapitola se zabývá dohledovým systémem na monitorování přenášených dat počítačovou sítí. Na závěr této bakalářské práce jsou uvedeny znalosti a zkušenosti získané během odborné praxe a celkové zhodnocení.

Klíčová slova

počítačová síť; směrovač; přepínač; monitorovací systém; analýza

Abstract

This bachelor thesis describes the course of passing the individual professional practice in Výzkumný ústav vodohospodářský T. G. Masaryka v.v.i. In this thesis describe the analysis of the current situation of the computer network and then proposal a new computer network to facilitation administration. The last chapter deals with the surveillance system to monitoring data transmitted by computer network. At the conclusion this bachelor thesis are given the knowledge and experience gained during individual professional practice and overall evaluation.

Key words

computer network; router; switch; monitoring system; analysis

Seznam použitých zkratek

Zkratka	Anglický význam	Český význam
ARP	Address Resolution Protocol	Protokol sloužící k získání linkové adresy síťového rozhraní
DAI	Dynamic ARP Inspection	Dynamická prohlídka ARP paketu
DHCP	Dynamic Host Configuration Protocol	Protokol pro dynamickou konfiguraci hosta
FTP	File Transfer Protocol	Protokol pro přenos souborů
HTTP	Hypertext Transfer Protocol	Protokol pro výměnu hypertextových dokumentů
IP	Internet Protocol	Internetový protokol
LAN	Local Area Network	Místní síť
MAC	Media Access Control	Identifikátor síťového rozhraní
SSH	Secure Shell	Šifrované připojení uživatelského rozhraní
PC	Personal Computer	Osobní počítač
QoS	Quality of Service	Rezervace a řízení datových toků
RRDTool	Round-Robin Database Tool	Nástroj na zpracování a ukládání časově závislých dat
STP	Spanning tree protokol	Protokol k odstranění smyček v síti
UTP	Unshielded Twisted Pair	Nestíněná kroucená dvojlinka
VLAN	Virtual Local Area Network	Virtuální lokální síť

Obsah

1 Úvod

Vykonání odborné praxe ve firmě jako formu zpracování bakalářské práce jsem se rozhodl z důvodu prohloubení vlastních zkušeností a znalostí a získání nových poznatků o fungování firemních standardů, které jak doufám, budou přínosem pro mou budoucí kariéru.

Bakalářská práce se zaobírá především analýzou, návrhem a monitoringem firemní sítě LAN.

První kapitola popisuje odborné zaměření výzkumného ústavu a popis mého pracovního zařazení ve firmě.

V druhé kapitole nalezneme zadání a požadavky jednotlivých úkolů.

V kapitole 4.1 je popis mého postupu při samostatném seznámení s firemní počítačovou sítí LAN. Popis použitých programů pro analýzu počítačové sítě a jejich výstup. Dále jsou popsány funkce a možnosti jednotlivých aktivních a pasivních prvků ve stávající počítačové síti LAN.

Kapitola 4.2 se zabývá návrhem nové počítačové sítě LAN dle zadání. V prvních odstavcích popisuji seznámení se směrovačem MikroTik 750GL a vytvoření testovací sítě. V dalších odstavcích je popis rozdělení IP adres mezi zařízení, návrhy topologií a použití stávajících zařízení s využitím možností aktivních prvků pro lepší správu a přehled na počítačovou LAN sítí.

V kapitole 4.3 popisuji především instalaci a nastavení monitorovacího systému Cacti a nastavení SNMP protokolu na počítači s operačním systémem Windows 7 Professional.

V závěru této bakalářské práce shrnuji znalostí a zkušeností, které jsem získal v průběhu studia, a které jsem uplatnil při odborné praxi. Dále pak poznatky a nabité zkušenosti, hodnocení průběhu odborné praxe a dosažené výsledky.

2 Odborné zaměření firmy

2.1 Odborné zaměření firmy

Odbornou praxi jsem vykonával ve Výzkumném ústavu vodohospodářském T. G. Masaryka, v.v.i. pobočka Ostrava, který zkoumá užívání a změny vodních ekosystémů a jejich vazeb v krajině a souvisejících environmentálních rizik. Dále pak nabízí odbornou podporu ochrany vod, protipovodňové prevence a hospodaření s obaly a odpady.

2.2 Popis pracovního zařazení

Mé zařazení ve výzkumném ústavu bylo na oddělení informatiky a provozu pobočka Ostrava, které spravuje firemní počítačovou síť, upravuje a rozvíjí standardní i specializované programy, databázové a informační systémy a následně jejich aplikaci v oblasti vodního hospodaření. V neposlední řadě se oddělení stará o vedení operativní agendy pobočky a zabezpečuje technický chod pobočky.

3 Zadané úkoly v průběhu odborné praxe

3.1 Seznámení se s pracovištěm, analýza počítačové sítě

Seznámit se s firemní politikou a chodem firmy. Analyzovat současný stav firemní počítačové sítě LAN, zjistit parametry a funkce aktivních prvků v síti jako jsou přepínače a směrovače a vytvořit seznam služeb, které nabízí současná počítačová LAN síť. Výstupem analýzy je vytvoření schématu zapojení firemní LAN sítě, zařízení poskytující služby pro chod sítě a pro zaměstnance firmy, popis funkcí a protokolů, které nabízejí aktivní prvky v síti.

Na výše uvedené úlohy je 10 pracovních dnů.

3.2 Návrh nové počítačové sítě

Návrh počítačové LAN sítě s použitím stávajících zařízení zjištěných při analýze počítačové sítě v prvním úkolu s využitím funkcí aktivních prvků pro lepší správu a přehlednost nad počítačovou sítí. Pro nový adresní prostor je IP adresa sítě 192.168.49.0 s maskou 23. V návrhu počítačové sítě LAN lze navíc použít směrovač Router Board MikroTik 750 GL.

Návrh musí splňovat několik podmínek:

- Bude-li to možné, budou datové zásuvky označené písmenem D v kancelářích sloužit pouze pro LAN síť a telefonní zásuvky označené písmenem T pouze pro telefony. Nepoužívané zásuvky budou deaktivovány na přepínačích, případně vypojeny z přepínačů.
- DHCP server přidělí IP adresu většině zařízení v sítí na základě MAC adresy, s výjimkou serverů, firewallu, NAS disků a počítače správce sítě. Tyto zařízení budou mít IP adresy nastaveny ručně.
- Adresní prostor logicky rozdělit dle CIDR na několik rozsahů. Například od IP adresy 192.168.48.1 do 192.168.48.30 se budou nacházet servery.

Jelikož se jedná o klíčovou část, není určena maximální doba práce na těchto úlohách. Úkol však musí být hotový do konce odborné praxe.

3.3 Monitorovací systém sítě

Návrh sběru informací o zatíženosti síťových linek například pomocí protokolu SNMP. Možnost využití některého z dostupných monitorovacích systému běžících buď to pod operačním systémem Windows, nebo některou distribucí Linuxu.

Na návrh a nalezení vhodného monitorovacího systému je 6 pracovních dnů.

4 Postup řešení zadaných úkolů

4.1 Seznámení se s pracovištěm, analýza počítačové sítě

Při zahájení odborné praxe jsem se seznámil s pracovním prostředím, strukturou a politikou firmy, se softwarem na emailovou a firemní komunikaci.

Prvním úkolem bylo samostatné seznámení s aktuální firemní počítačovou sítí LAN, zjištění běžících služeb a analýza síťových uzlů a koncových zařízení, pomocí přiděleného počítače a volně dostupného softwaru. Na přidělený počítač jsem nainstalovat operační systém Windows 7 Professional s firemní licencí. Z příkazového řádku počítače jsem si zjistil přidělenou IP adresu DHCP serverem, bránu, a doménu. Proxy servery jsem si nastavil ručně dle pokynů správce sítě.

Abych při hledání zařízení v sítí nemusel ručně zjišťovat, která zařízení jsou připojená v síti pomocí programu ping a nslookup v příkazovém řádku počítače, použil jsem specializované programy. Jedním z nich byl Advanced IP scanner a druhý Angry IP scanner. Stáhnout si je lze oficiálních webových stránek [1] [2]. Oba nástroje dle nastaveného rozsahu IP adres zjistí, která zařízení se nachází na síti LAN, jejich doménové jméno a fyzickou adresu. Tyto nástroje dále disponují funkci skenování portů daného zařízení. Takže nám navíc zjistí, zda na zařízení neběží nějaká služba jako například HTTP nebo FTP. Program se bude snažit oskenovat nejznámější porty jako například 20 a 21 (FTP), 80 (HTTP), 443 (HTTPS) a to navázáním spojení. Je však možné, že firewall daného zařízení bude žádosti o navázání spojení zahazovat a výsledky tak mohou být neúplné. Některé zjištěné služby jsem si mohl ověřit. Například jsem se mohl připojit přes klienta na FTP server, nebo otevřít webové stránky v prohlížeči.

Další nástroj, který jsem použil, byl Zenmap. Je to grafická nástavba využívající známý program nmap. Zenmap nám dokáže stejně jako výše uvedené programy ověřit dostupnost zařízení a otevřenost portů, navíc dokáže mnohdy odhalit operační systém, či přítomnost firewallu. Na oficiálních stránkách programu Zenmap [3] nalezneme kromě samotného programu i dokumentaci.

V dalším kroku jsem vycházel z dokumentu seznam zařízení v síti, který mi poskytl správce sítě. V dokumentu jsem si mohl ověřit správnost zjištěných informací, doplnit si zařízení, které jsem uvedenými postupy nenašel a dopsat zařízení, která v seznamu nebyla uvedena.

Mezi zjištěnými službami byl DHCP server pro přidělování IP adres, DNS server pro překlad doménových jmen, tři disková pole NAS, dvanáct síťových tiskáren s webovým rozhraním, server pro emailovou komunikaci a firewall. Dále se na síti nacházelo 21 osobních počítačů a dva WiFi směrovače.

O aktivních prvcích, které jsou použité ve firemní LAN síti, jako je firewall, přepínače a rozbočovač jsem si zjistil typ zařízení a poté jsem si na internetu vyhledal dokumentaci, ze které jsem vyčetl parametry, postupy nastavení a podporované protokoly a technologie.

Firewall SOPHOS UTM 110/120 nabízí velkou škálu funkcí a ve firemní LAN síti sloužil jako směrovač a brána do internetu. Toto zařízení obsahuje 4 gigabitové LAN porty, podporuje například překlad adres NAT, filtrování URL, virtuální privátní síť (VPN), má ochranu proti malware, ochranu proti spamu, prevence útoku DoS a systém prevence průniku IPS. Firewall SOPHOS nabízí velkou škálu funkcí a nastavení, čímž se stává dobrou ochranou firemní počítačové LAN sítě. Společnost SOPHOS navíc nabízí zdarma software s názvem SOPHOS UTM Home Edition, který si můžeme nainstalovat například jako virtuální počítač a testovat jeho funkce, nebo jej nasadit do malé počítačové sítě LAN jako firewall. Více informací o SOPHOS firewall se dočtete na oficiálních stránkách výrobce [4] a z dokumentace [5]. Mým úkolem nebylo se dopodrobna zabývat tímto zařízením, pouze se s ním seznámit a mít o něm nějaké povědomí.

Přepínač Zyxel GS 2200-24 má 24 gigabitových LAN portů a 4 gigabitové duální LAN porty. Nabízí management a řízení toku dat QoS. Nastavovat je lze přes webové rozhraní, nebo přes SSH. Nabízí velké množství protokolů a technologií pro řízení a zabezpečení provozu. Pouze některé se budou hodit při návrhu nové počítačové LAN sítě, jako například: STP, VLAN, SNMP a Agregace linek. Ještě zmíním možnost filtrování MAC adres na portech jako další zabezpečovací prvek tohoto přepínače. Popis jednotlivých technologii a protokolů je uveden níže. Podrobnější informace jsou uvedeny v dokumentaci [6] [7].

Přepínač 3COM BASELINE 2924 je obdobou přepínače Zyxel. Co do počtu portů, používaných technologií a protokolů jsou shodné. Více informací v oficiální dokumentaci [8].

Přepínač NETGEAR GS724TPS má 24 gigabitových LAN portů. Nabízí management a řízení toku QoS. Nastavovat je lze přes webové rozhraní, nebo SSH. Oproti výše uvedeným přepínačům nabízí více technologií, které můžeme použít při návrhu nové počítačové LAN sítě. Kromě již zmíněných protokolů a technologií u přepínačů výše nabízí technologii DHCP Snooping a technologii DAI. Obě technologie jsou popsány níže. Dokumentaci k tomu přepínači nalezneme na podpoře výrobce [9].

Dále se v sítí nacházeli přepínače TLSG 2216 web a 3COM BASELINE 2824. Oba přepínače obsahovali základní technologie a protokoly pro jejich funkci, neměli možnost managementu a nenabízeli technologie a funkce, které bychom mohli využít při návrhu nové počítačové LAN sítě. Bližší informace nalezneme na webových stránkách [10] a [11].

STP (Spanning Tree Protocol) je síťový protokol, který odstraňuje mezi přepínači smyčky. Přepínače s tímto protokolem umí zjistit topologii sítě a odpojit redundantní spoje, které v sítí způsobují například množení broadcastů a tím zahlcení sítě. Protokol také umí znovu automaticky aktivovat odpojené spoje v případě, že dojde k přerušení aktivní cesty. Další informace k protokolu jsou na webových stránkách [12].

VLAN (Virtual Local Area Network) technologie slouží k logickému rozdělení sítě. Díky managementu přepínače můžeme vytvořit několik VLAN sítí a k nim přiřadit porty přepínače. Můžeme tak docílit toho, že dvě sítě budou od sebe rozděleny na jednom přepínači a komunikace mezi nimi bude možná přes směrovač. Bližší informace nalezneme na [13].

SNMP (Simple Network Management Protokol) je protokol aplikační vrstvy. Slouží pro potřeby správy sítě. Umožňuje sběr nejrůznějších dat jako je například stav zařízení (zapnuto, vypnuto), zatížení harddisku, teplota procesoru, zatížení LAN portů, stav barev tiskárny a mnoho dalšího. Tento protokol je transakčně orientovaný na modelu klient - server. Na klientovi běží agent, který odpovídá na požadavky serveru. Na serveru běží manažer, který sbírá data. Agent může data vysílat i na základě předem definované situace. Spoustu dalších informací k tomuto protokolu jsou uvedeny na webových stránkách [14] a [15].

DHCP Snooping je technologie, díky níž zabráníme komunikaci DHCP serveru s hosty, který na sítí nemá co dělat. Na přepínači v nastavení DHCP Snooping nastavíme port, na který máme připojený náš DHCP server jako "trusted" (důvěryhodný). Na ostatní porty, kde jsou připojené například počítače a tiskárny, nastavíme "untrusted" (nedůvěryhodný). V případě, že připojujeme k přepínači další přepínač, který také tuto technologii má a je zapnutá a nastavená, můžeme na daný port nastavit "trusted", v opačném případě nastavíme "untrusted". Po nastavení přepínače bude na DHCP žádosti odpovídat pouze DHCP server připojený na port s nastavením "trusted". DHCP Snooping navíc vytváří tabulku z informací získaných při žádostech o přidělení IP adresy DHCP serveru. V tabulce se nacházejí informace o fyzické adrese zařízení MAC, přidělené IP adrese, port, na kterém se klient nalézá, dobu, kdy vyprší zapůjčení IP adresy, VLAN, do které klient spadá a způsob, jak bylo položka přidána. Tabulku můžeme vidět na obrázku 4.1. Další informace lze nalézt na webových stránkách [16] a [17].

MAC Address	IP Address	Expires(s)	VLAN	Port ID	Source
00-05-36-b2-8d-7d	192.168.48.10	120	2	10 5	Dynamic

Obrázek 4.1: Záznam vytvořený technologii DHCP Snooping

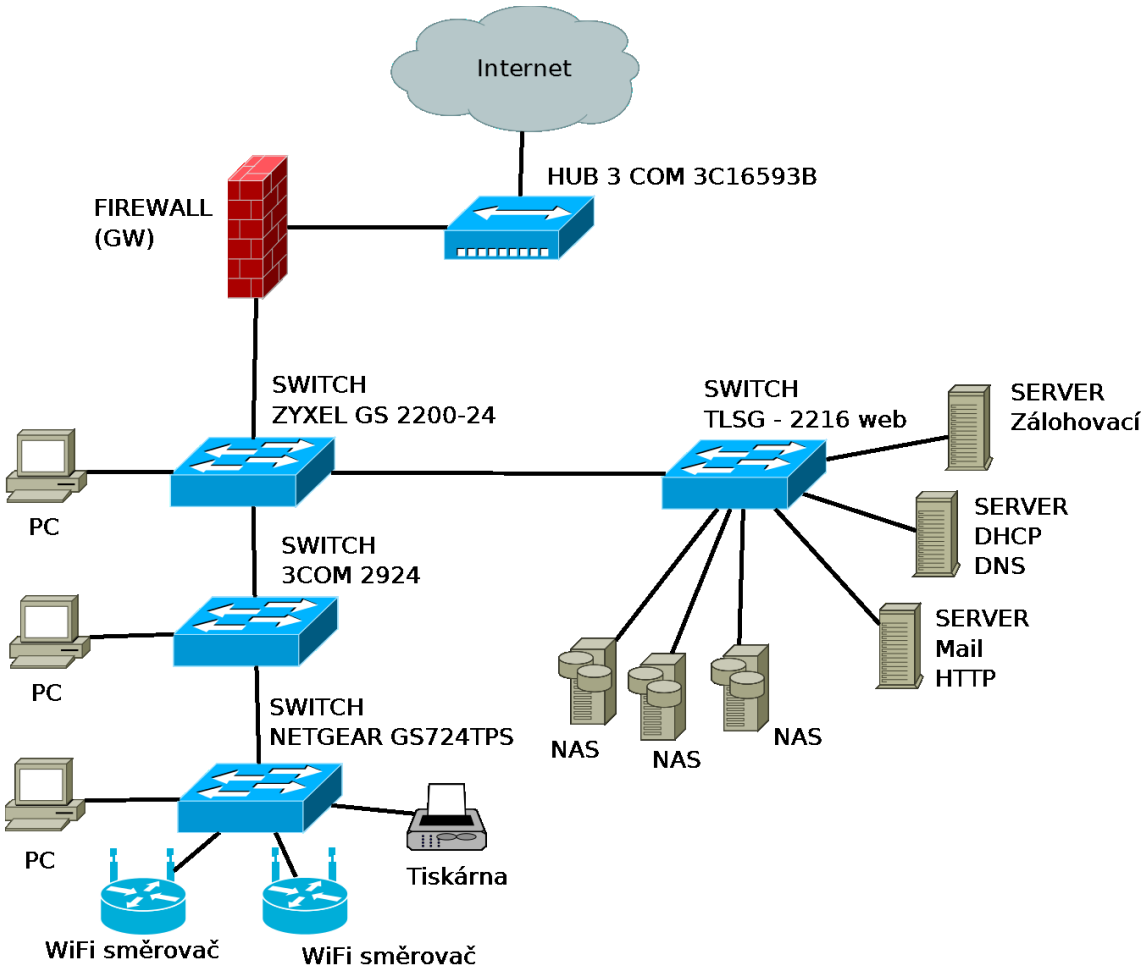
DAI (Dynamic ARP Inspection) je technologie, která využívá tabulku vytvořenou při DHCP Snoopingu. ARP protokol je důležitým protokolem pro provoz IPv4 sítě, který nám zjišťuje, jaká je fyzická MAC adresa zařízení, když známe IP adresu. Technologie DAI kontroluje ARP pakety přicházející z portů, na kterých je v DHCP Snoopingu nastaveno "untrusted", zda k sobě patří MAC adresa a IP adresa počítače žádajícího o zjištění MAC adresy. V případě ARP Reply (ARP odpověď) se navíc kontroluje, zda k sobě patří MAC a IP adresa počítače odpovídajícího na ARP Request (ARP dotaz). Pokud k sobě MAC adresa a IP adresa nepatří, je ARP paket zahozen. Pokud máme v počítačové síti LAN zařízení, které má statickou IP adresu, lze záznam vytvořit v tabulce DAI Access List ručně. Pokud není DHCP Snooping aktivní, technologie DAI využívá tabulku DAI Access List. O technologii DAI a o útocích na přepínače je napsaný článek na webových stránkách [18].

Agregace linek je termín, který se používá, chceme-li zvýšit propustnost počítačové sítě. Na přepínačích můžeme použít například dva porty pro připojení jednoho zařízení, ke kterému přistupuje velké množství uživatelů. Toto zařízení musí mít dvě síťové karty a nastavený NIC Teaming. Takovéto propojení může být i mezi dvěma přepínači, které podporují technologií agregaci linek. Další informace na webových stránkách [19].

Rozbočovač 3 COM BESELINE DUAL SPEEDHUB slouží k připojení internetu od poskytovatele. Jeho propustnost je 100 Mbit/s.

Typ LAN kabelů je UTP kategorie CAT 5e, 1 Gbit/s a šířkou pásma 100 MHz.

Po analýze jsem vytvořil schéma zapojení počítačové sítě LAN. Na obrázku 4.2 je zobrazené zjednodušené schéma pro lepší přehlednost. Nevýhodou stávající sítě bylo dosud nevyužívání managementu přepínačů a tím technologií a protokolu, které by mohli zpřehlednit LAN síť pro správce sítě.



Obrázek 4.2: Zjednodušené schéma současné firemní LAN sítě

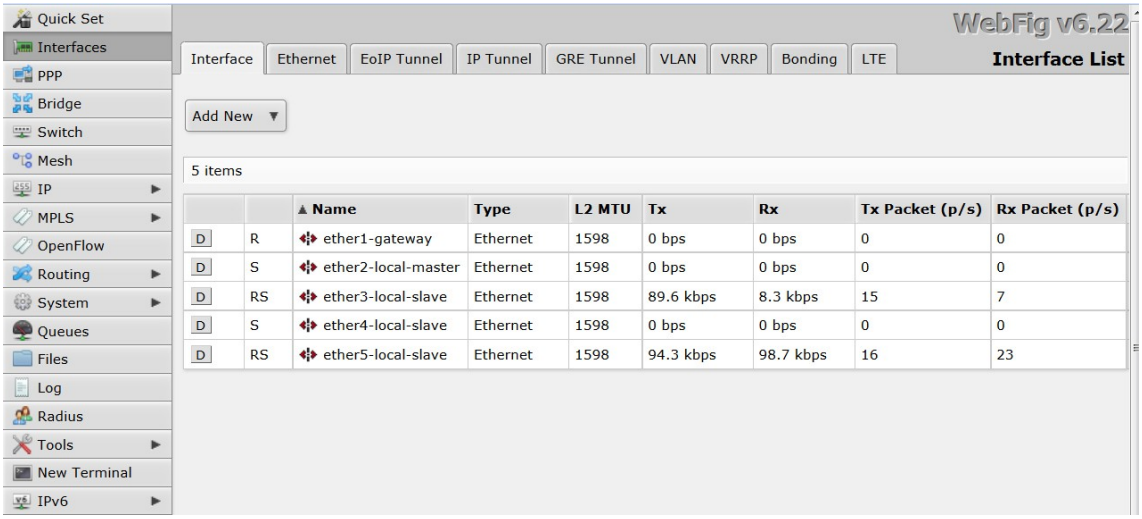
4.2 Návrh nové počítačové sítě

Při návrhu nové počítačové sítě LAN jsem vycházel z informací zjištěných při analýze sítě. V prvním kroku jsem se seznámil se směrovačem MikroTik typ 750 GL, který jsem mohl použít při návrhu nové počítačové LAN sítě.

Směrovač Mikrotik 750 GL nabízí velkou škálu možností a nastavení. Je to poměrně malé zařízení, které má 5 gigabitových LAN portů. Nabízí funkce jako DNS server, DHCP server, překlad adres NAT a filtrování provozu pomocí pokročilého firewallu. Umí také

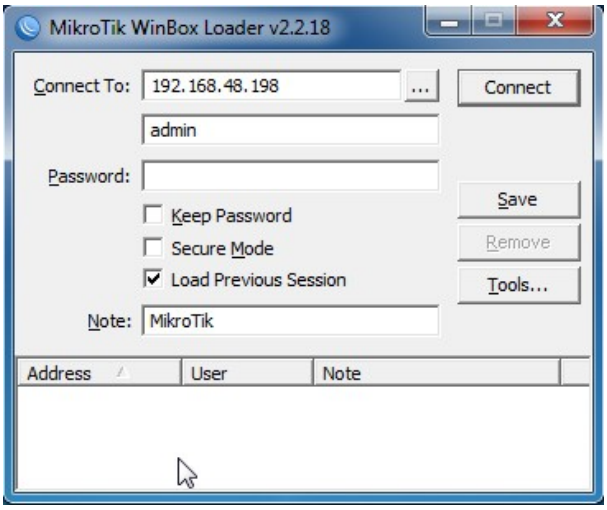
pracovat jako přepínač. Specifika směrovače nalezneme na webových stránkách [20]. O směrovačích MikroTik se lze dočíst na oficiálních webových stránkách [21], kde nalezneme dokumentaci a návody k nastavení všech funkcí.

Nastavovat jej lze přes webové rozhraní WebFig, nebo pomocí programu WinBox. Obě možnosti nabízí stejné funkce i přístup k příkazovému řádku. Na obrázku 4.3 můžeme vidět výřez prostředí ve webovém prohlížeči.

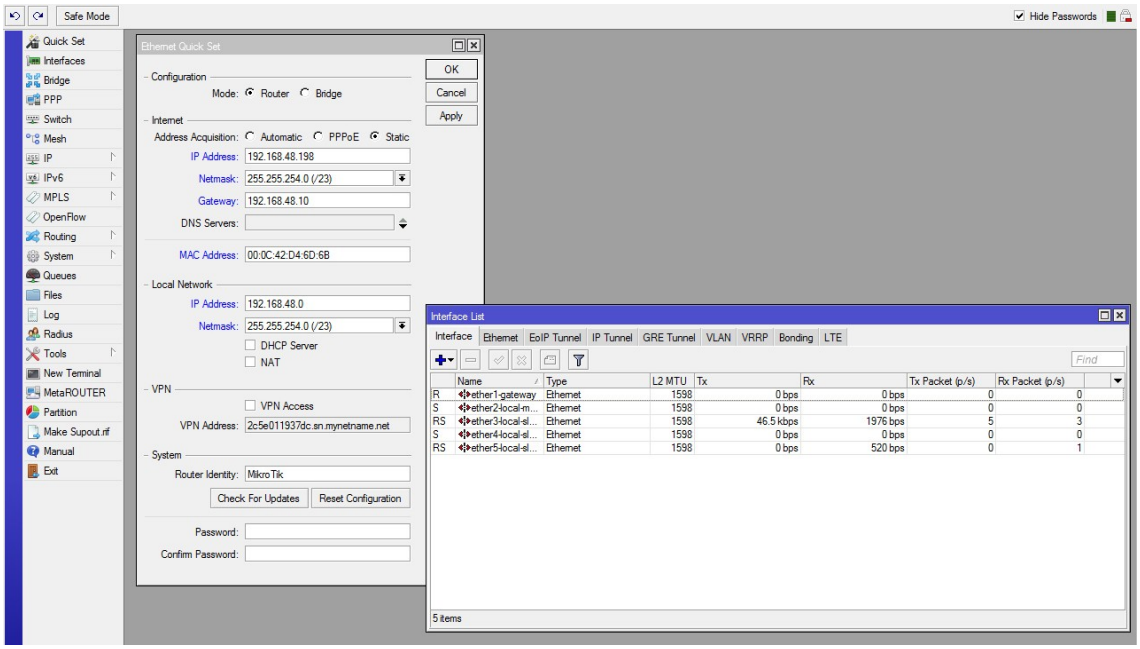


Obrázek 4.3: Webové rozhraní MikroTik

WinBox je program, který umí vyhledat zařízení MikoTik sám, pokud je takové zařízení připojené do sítě. Abychom se k zařízení MikroTik mohli připojit, musíme znát IP adresu zařízení, nebo MAC adresu. Na obrázku 4.4 je znázorněné přihlašovací okno programu WinBox. Na obrázku 4.5 pak prostředí programu WinBox, které je téměř shodné s webovým rozhraním.

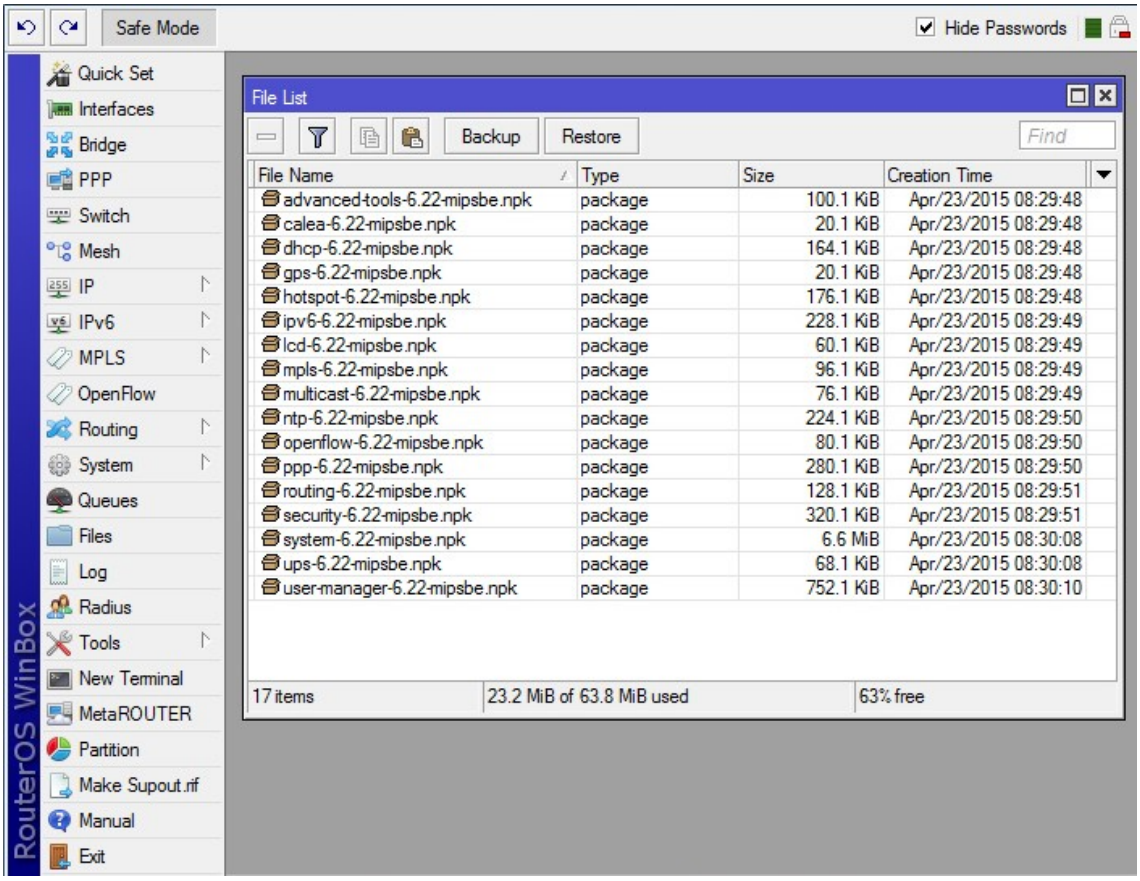


Obrázek 4.4: Přihlašovací okno WinBox



Obrázek 4.5: Prostředí WinBox

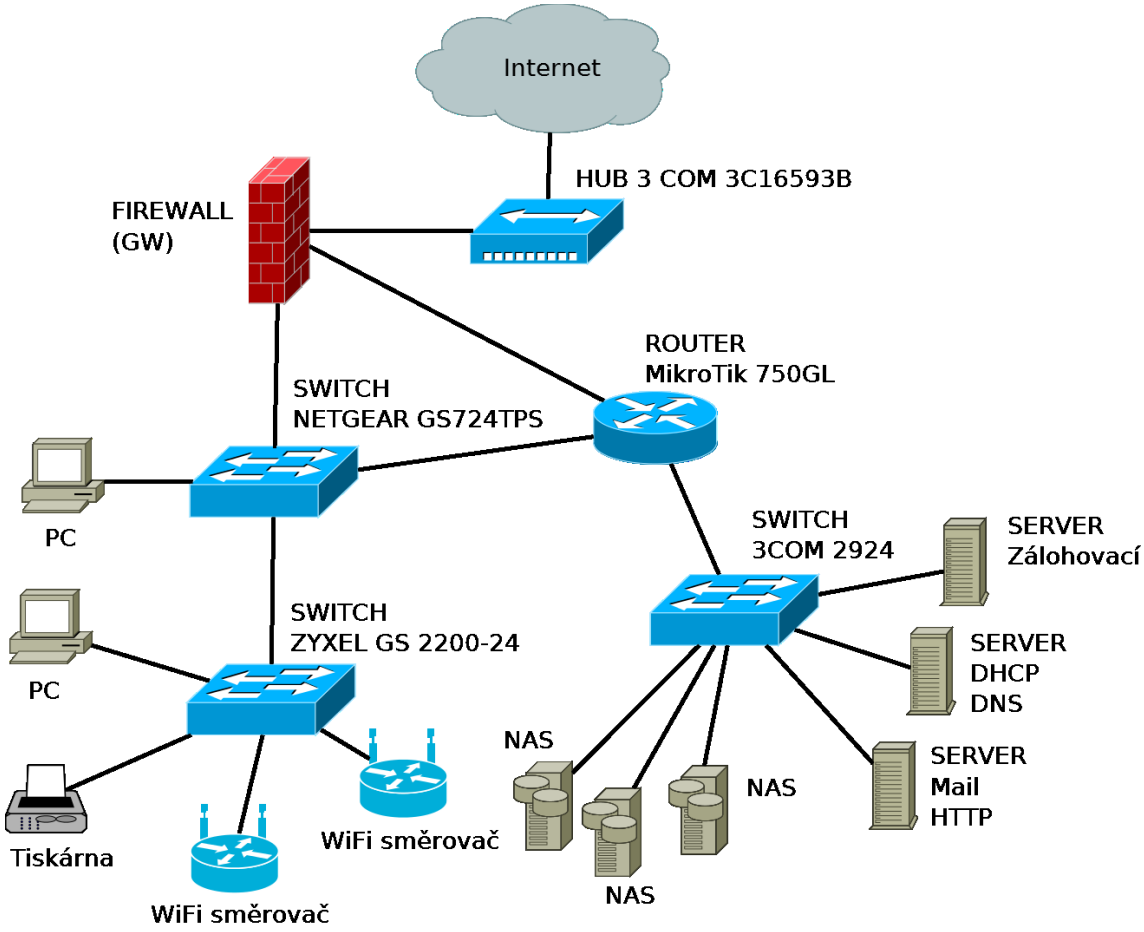
V prvním kroku jsem aktualizoval operační systém MikroTik. Stačilo stáhnout z oficiálních stránek aktuální balíčky, které jsem pomocí programu WinBox nakopíroval do importu souborů. Na obrázku 4.6 je vidět otevřený File List v programu WinBox, kam se balíčky přetáhnutím myší z počítače nakopírují.



Obrázek 4.6: File List WinBox

Jakmile jsou balíčky nakopírované, restartujeme směrovač (Systém - Restart). Je dobré zkontrolovat nainstalované balíčky, zda jsou všechny a zda nejsou některé zbytečné. Například MikroTik 750GL nenabízí WiFi, takže je zbytečné mít balíček wireless pro WiFi nainstalovaný. Po opětovném spuštění je již MikroTik aktualizovaný.

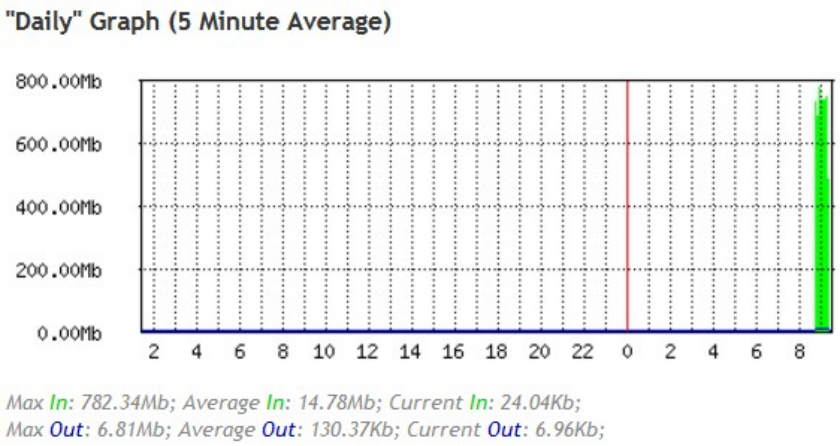
V prvním návrhu topologie sítě má směrovač MikroTik sloužit jako brána mezi uživateli a servery jak je zobrazeno na obrázku 4.7. Obrázek znázorňuje pro větší přehlednost zjednodušené schéma návrhu. Nejsou uvedena všechna koncová zařízení. Uživatelé se nacházejí v síti 192.168.48.0/24, servery a NAS disky se nacházejí v síti 192.168.49.0/24.



Obrázek 4.7: Zjednodušený návrh topologie s použitím směrovače MikroTik

Pro otestování návrhu topologie jsem si vytvořil testovací síť, abych si ověřil funkčnost a nastavení směrovače. Testovací síť obsahovala dva servery. Na jednom byl spuštěn DHCP server s Windows server 2008 R2 a druhý server s operačním systémem Debian sloužil k testování. K testovací síti jsem se připojil se svým počítačem s operačním systémem Windows 7 Professional a počítačem s operačním systémem Ubuntu, který jsem měl nainstalovaný ve virtuálním prostředí na svém počítači. K serverům jsem se připojil přes SSH nebo přes připojení ke vzdálené ploše. Testoval jsem zatížení směrovače MikroTik při přenášení velkých souborů, ze serveru na můj počítač a nastavení farewallu.

Na obrázku 4.8 je zobrazen graf měření přenášených dat zobrazený přes webové rozhraní.



Obrázek 4.8: Graf přenášených dat

Během testování jsem však neměl ponětí o tom, kolik dat se skutečně přesouvá po firemní LAN síti. Z tohoto důvodu jsem se začal zaobírat tím, jak monitorovat stav zatížení současné sítě. Na internetu jsem nalezl několik volně dostupných monitorovacích systémů, které lze použít. Více se o monitorovacích systémech zabývá kapitola: 4.3. Z výsledků monitorování bylo však patrné, že šířka využitelného pásma současné LAN sítě není ani zdaleka využita. Hodnoty se pohybovaly maximálně v desítkách megabitů za sekundu.

Při debatě se správcem sítě o potřebách přístupů uživatelů k serverům, jsme došli k závěru, že pokud se na sítí bude nacházet server, ke kterému nemá mít uživatel přístup, bude zabezpečen jinak, například jménem a heslem, nebo firewallem přímo na serveru. Z tohoto důvodu není zapotřebí oddělovat servery od uživatelů další bránou (firewallem).

Druhý a výsledný návrh LAN sítě už s použitím směrovače MikroTik nepočítá. V návrhu nejsou použité přepínače, které nenabízí management. Síť má IP rozsah 192.168.48.0 a masku 23, tzn. první zařízení má IP adresu 192.168.48.1 a poslední 192.148.49.254.

Adresní prostor jsem rozdělil dle CIDR na několik kategorií. CIDR se používá na rozdělení sítě na podsítě zvolením masky sítě pro každou podsíť, která tak definuje rozsah IP adres. Doplňující informace jsou na webových stránkách [22]. Díky tomuto rozdělení bude jednodušší nastavení firewallu a adresní prostor se stane přehlednější. Maska sítě dle CIDR nám určí pouze logický rozsah. Skutečná maska sítě zahrnuje celou síť (maska 23) nebo polovinu naší sítě (maska 24). Zařízení jako servery, NAS disky a firewall má nastavenou masku 23, ostatní zařízení v síti mají masku 24. Toto rozdělení bylo na žádost správce sítě. Tabulka 1.1: popisuje rozdělení IP adres dle zařízení a znázorňuje jednotlivé kategorie a k nim rozsah IP adres.

Tabulka 1.1: *Rozdělení IP adres dle zařízení*

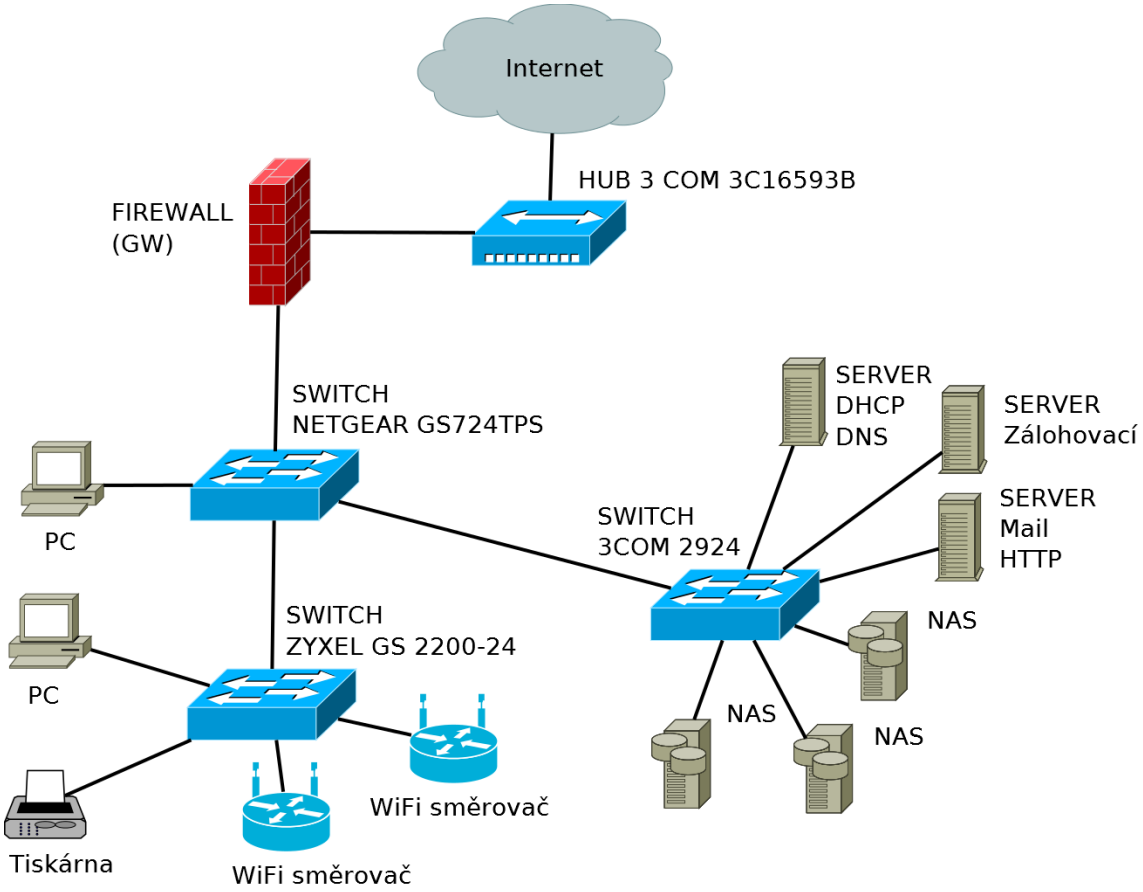
Zařízení	Počáteční IP adresa	Koncová IP adresa	Maska
Servery	192.168.48.1	192.168.48.30	23
Brána/firewall	192.168.48.33	192.168.48.34	23
NAS	192.168.48.48	192.168.48.62	23
Tiskárny	192.168.48.65	192.168.48.94	24
WiFi	192.168.48.105	192.168.48.110	24
Ostatní zařízení	192.168.48.113	192.168.48.126	24
Uživatelská PC	192.168.48.129	192.168.48.190	24

Všechny přepínače využívají protokol STP a SNMP. Technologii DHCP Snooping využívá přepínač NETGEAR, ke kterému je připojen přepínač se servery, kde je mimo jiné i DHCP server.

Původně bylo v plánu nastavit na DHCP serveru několik rozsahů s názvem zařízení, které do něj spadají. Na DHCP serveru Windows 2008 R2 však nelze nastavit více rozsahů v rámci jedné sítě se stejnou maskou. Nabízela se dvě řešení. První spočívalo v nastavení rozsahu DHCP serveru pouze pro uživatele a ostatní zařízení nastavit ručně. Druhé řešení spočívalo v nastavení rozsahu DHCP serveru pro všechna zařízení, které budou mít masku 24 a spadají do sítě 192.168.48.0, kam patří uživatele, tiskárny, přepínače a WiFi. Zařízení jako servery, disková pole NAS a firewall, s maskou 23 by byla nastavena ručně. Rozhodl jsem se pro druhou variantu. V nastavení DHCP jsem vytvořil obor pro síť 192.168.48.0 s maskou sítě 24. Poté jsem nastavil rezervování IP adres na základě MAC adres. Aby se nemohlo stát, že nové zařízení, které připojíme do sítě, dostalo IP adresu, bez toho, aby bylo rezervované na DHCP serveru, vyjmul jsem celý rozsah oboru. Dosáhl jsem tak toho, že IP adresu od DHCP serveru dostane pouze zařízení, které je rezervované.

Společně se správcem sítě proběhla kontrola datových a telefonních zásuvek v kancelářích, kde bylo potřeba zkontrolovat, které zásuvky se využívají a jaké zařízení je v nich zapojené. Nevyužívané zásuvky jsme vypojili z přepínačů.

Na obrázku 4.9 je zobrazen návrh topologie sítě, který byl realizován. Opět se jedná o zjednodušené schéma kvůli větší přehlednosti.



Obrázek 4.9: Zjednodušený schéma návrhu realizované počítačové sítě

4.3 Monitorovací systém sítě

S monitorováním počítačových sítí jsem doposud neměl žádné zkušenosti. V první řadě jsem si našel informace o tom, jakým způsobem monitorovací systémy počítačových LAN sítí fungují, co k tomu využívají a co všechno lze monitorovat. Obecně lze říci, že monitorovací systémy fungují na bázi manažer - agent. Manažer běží na serveru, který sbírá informace, ukládá je a může je i interpretovat například ve formě grafů. Agent běží na daném zařízení a poskytuje manažerovi potřebné informace. O informace si může manažer sám říct v definovaných okamžicích, nebo je agent poskytne s ohledem na nějakou událost. Velice dobře napsaný článek o monitoringu sítě je na webových stránkách [23] ze kterých jsem vycházel.

Pro monitoring sítě jsem využil protokolu SNMP (Simple Network Management Protokol). Jedná se o nejznámější protokol, který se používá k monitorování a správě sítě a síťových zařízení. Protokol SNMP je standardizovaný protokol aplikační vrstvy. Byl vyvinut s ohledem na rozvoj a rozšiřování počítačových sítí, tak aby umožňoval vzdálenou správu síťových prvků a podrobnější nepřetržitý dohled. Vývoj protokolu započal v roce 1988. V roce 1989 vychází první verze protokolu SNMPv1.

Druhá verze protokolu SNMP s označením SNMPv2 nebo také SNMPv2c vychází z první verze a mimo jiné je přidána kontrola doručení zprávy. Třetí verze SNMPv3 nabízí šifrování komunikace a to včetně ověření uživatele. Nejvíce zařízení podporuje druhou verzi SNMPv2. Podrobnější popis je na webových stránkách [14] a [15].

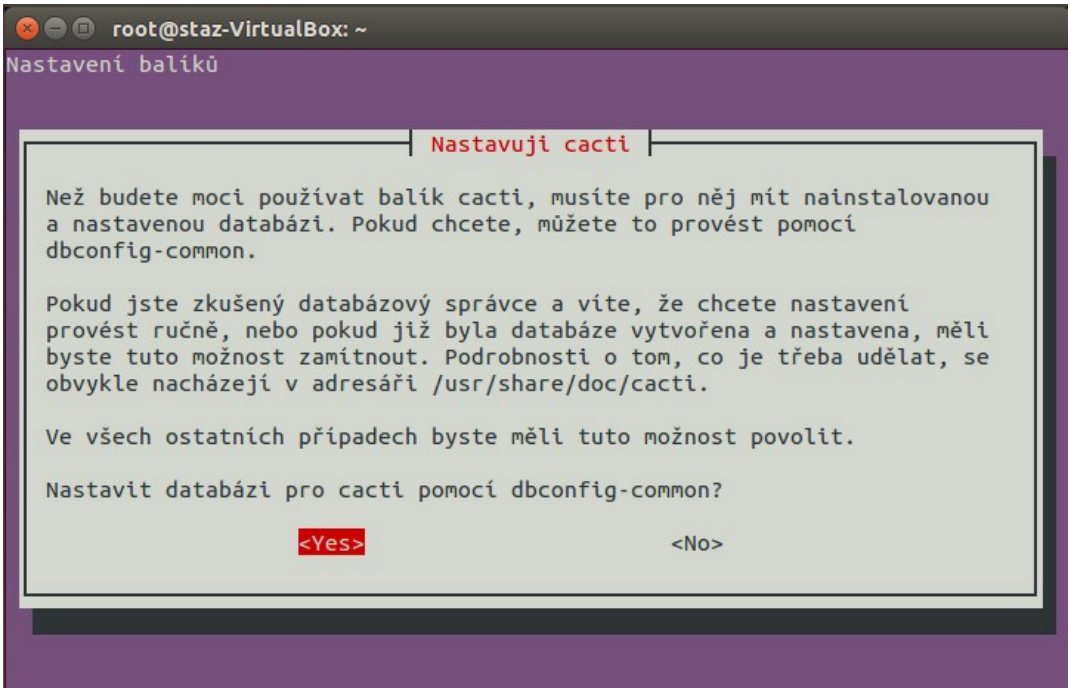
Při hledání vhodného manažera jsem narazil na několik systémů na monitorování počítačové sítě LAN. Zaměřil jsem se na volně dostupné systémy, ze kterých jsem následně vybral jeden, který jsem použil. Vybíral jsem mezi monitorovacími systémy Nagios, Zabbix a Cacti. Bližší informace ke všem třem systémům můžeme najít na oficiálních webových stránkách [24], [25] a [26], na kterých jsou uvedeny návody a rady.

Všechny tři uvedené systémy využívají protokol SNMP a nabízí to, co od nich požaduji tj. monitorování zatíženosti sítě aktivních prvků (přepínačů a PC s operačním systémem Windows nebo Linux). I když systém Nagios stejně jako Zabbix nabízí široké uplatnění, vybral jsem systém Cacti a to především s ohledem na jednoduchou instalaci a konfiguraci.

Monitorovací systém Cacti je nástroj zejména pro tvorbu grafů z dat, která shromažďuje z námi definovaných zařízení. Tato data ukládá do databáze. Správu obstarává webové rozhraní. Jedná se kompletní nástavbu k nástroji RRDTool. RRDTool je nástroj, který zpracovává časově závislá data. Popis nástroje nalezneme na webových stránkách [27].

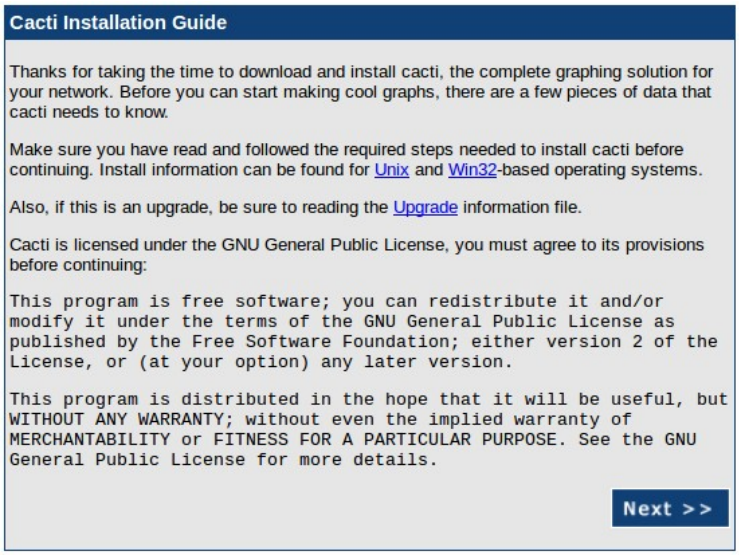
Instalace systému Cacti je poměrně jednoduchá. Následující instalace je popsána v operačním systému Ubuntu 14.04 64bit.

Před instalací systému Cacti jsem provedl aktualizaci a upgrade stávajících balíčků pomocí příkazu apt-get update a apt-get upgrade v terminálu. Také jsem nainstaloval webový server Apache 2. Následně jsem pomocí příkazu v terminálu apt-get install cacti zahájil instalaci. Instalace Cacti si vyžádala databázi jak je vidět na obrázku 4.10. Doposud nebyla žádná databáze nainstalována, takže jsem instalaci povolil. Vytvoření databáze si vyžádalo administrátorské heslo a heslo pro balík Cacti.



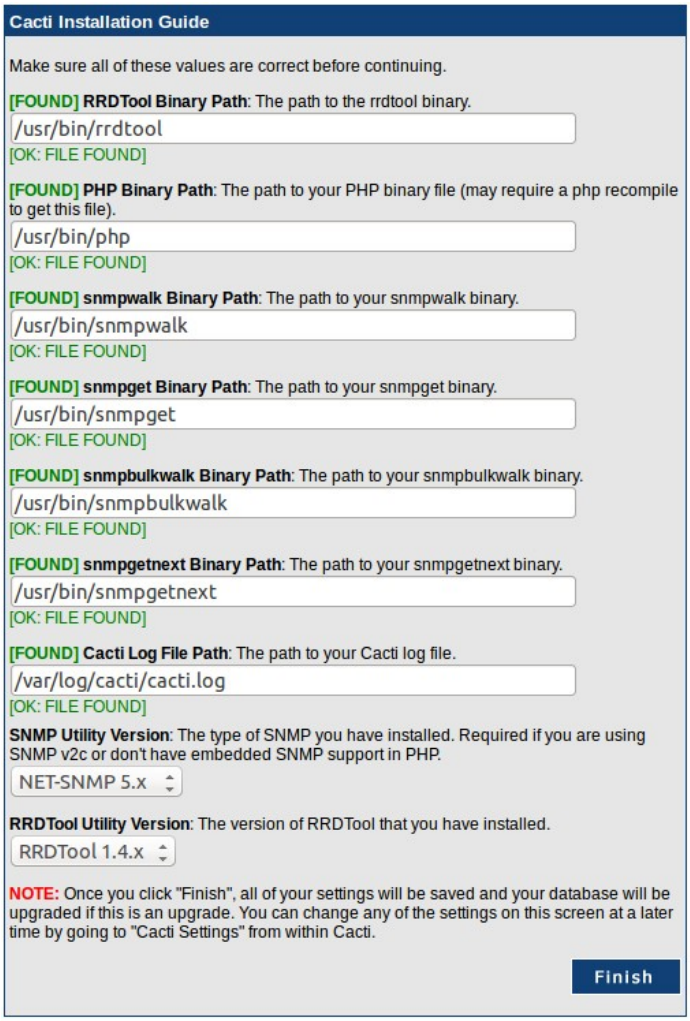
Obrázek 4.10: Nastavení databáze pro systém Cacti

V dalším kroku jsem nastavil webový server Apach 2. Instalace je tímto hotová. Zbývá už jen konfigurace systému Cacti. Otevřel jsem si webový prohlížeč a do adresního řádku napsal localhost/cacti. Na obrázku 4.11 je vidět průvodce instalací Cacti. V dalším kroku jsem vybral novou instalaci a pokračoval dále.



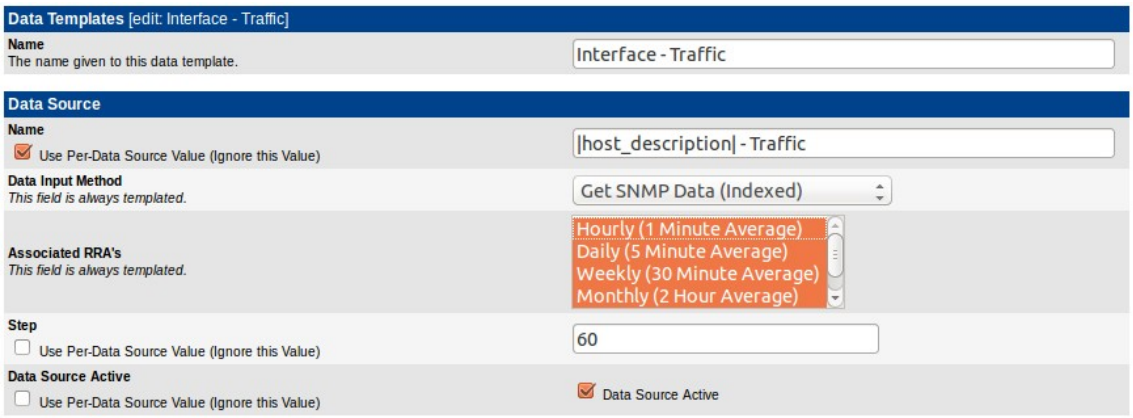
Obrázek 4.11: Uvítací okno průvodce instalací systému Cacti

Na obrázku 4.12 můžeme vidět, že všechny potřebné soubory byly nalezeny. Verzi SNMP Utility jsem nastavit na nejvyšší stejně jako verzi RRDTool Utility a pokračoval kliknutím na tlačítko Finish.



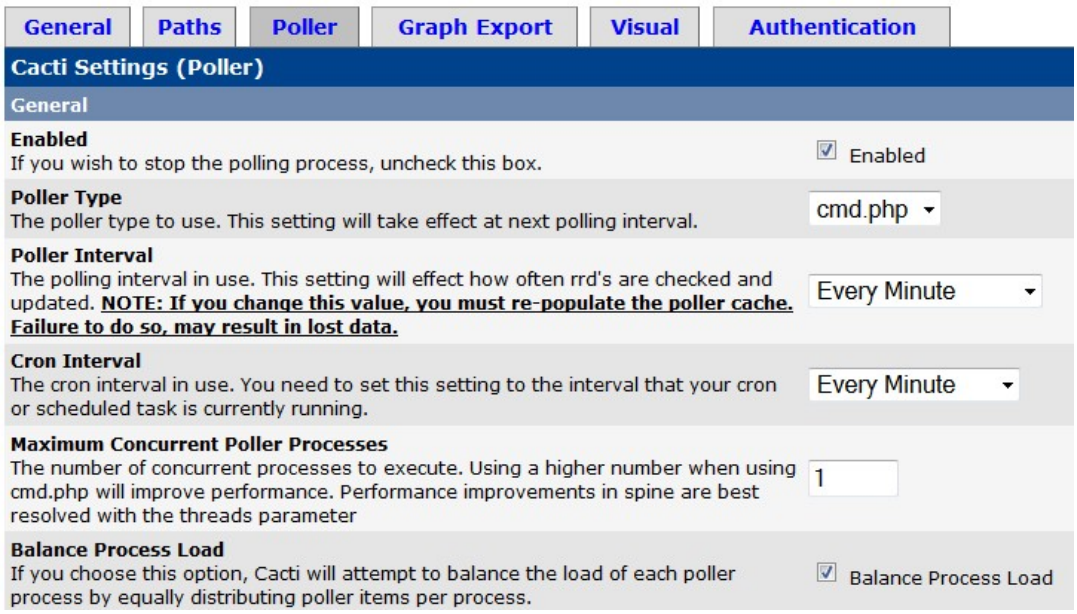
Obrázek 4.12: Kontrola nalezení potřebných souborů a nastavení verze SNMP Utility a RRDTool Utility

Zobrazilo se přihlašovací okno. Přihlašovací jméno je admin a heslo také admin. V dalším kroku si heslo můžeme změnit. Předtím, než jsem přidal první zařízení, nastavil jsem systém Cacti. Mým cílem bylo sledovat provoz na rozhraní zařízení s co největší přesností. Systém je teď nastavený pro sběr dat v intervalu pěti minut. Já jsem chtěl sbírat data v intervalu jedné minuty. V levém menu jsem kliknul na Data Templates a vybral Interface - Traffic. V sekci Data Source u Associated RRA's jsem přidal Hourly (1 Minute Average) jak zobrazuje obrázek 4.13 a změnil jsem krok (Step) z 300 sekund na 60 sekund. V záložce traffic_in a traffic_out jsem změnil Hearbeat z 300 sekund na 120 sekund dle doporučení z oficiálních stránek systému Cacti. Ostatní nastavení jsem nechal tak jak bylo.



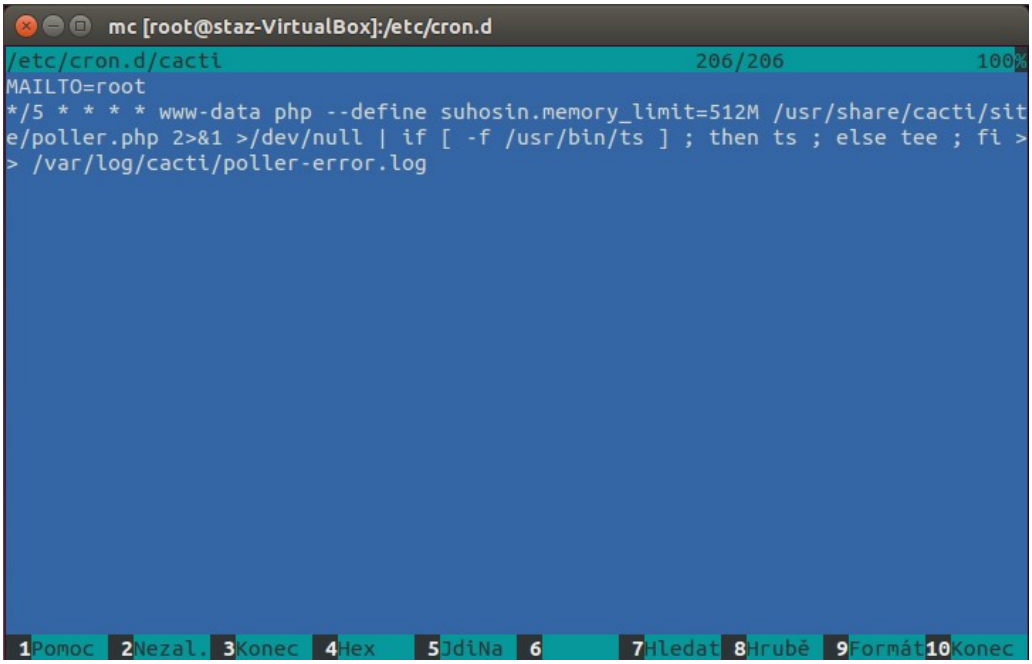
Obrázek 4.13: Nastavení sbírání dat v Interface - Traffic

Dále jsem se přemístil do nastavení (Setting v levém menu). V nastavení General jsem změnil SNMP verzi 1 na verzi 2 a název komunity nechal public. Další je nastavení Poller Interval a Cron Interval na záložce Poller, který jsem změnil z Every 5 Minutes na Every Minute. Nastavení je zobrazené na obrázku 4.14.

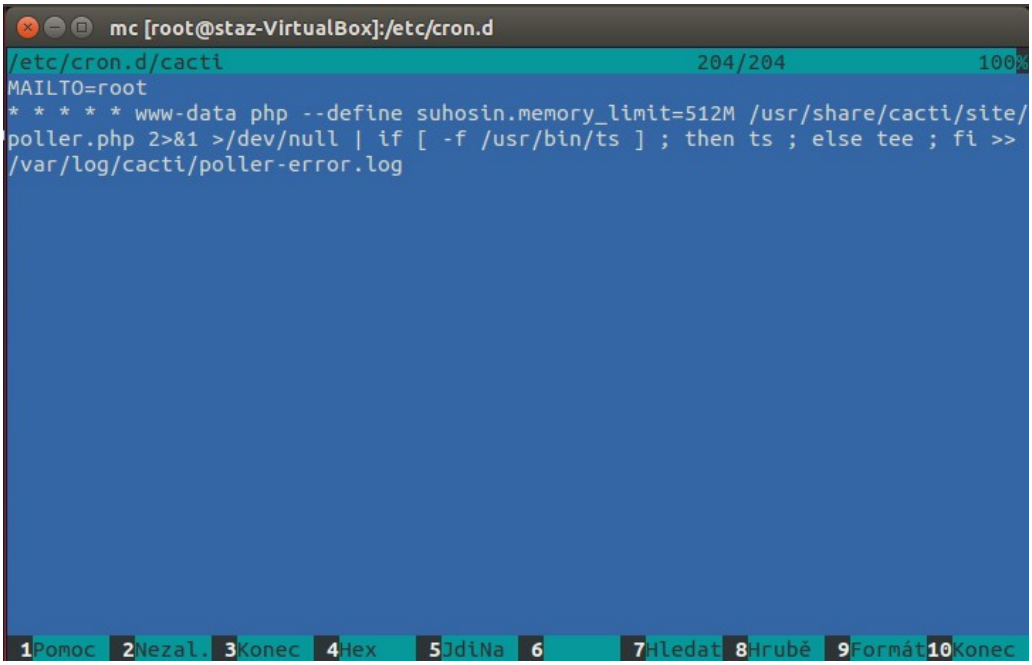


Obrázek 4.14: Nastavení časového intervalu

Poslední krok spočívá v nastavení souboru, který spouští démon Cron. Deamon Cron se používá k automatickému spouštění skriptů v určitý čas. Popis démona Cron je na webových stránkách [28]. Pomocí příkazu v terminálu nano /etc/cron.d/cacti jsem upravil soubor. Na obrázku 4.15 je původní nastavení souborů, kde je nastaveno spouštění v pěti minutových intervalech. Lomítko znázorňuje spouštění skriptu v intervalech a číslice za ní určuje interval. Úprava souboru spočívá ve smazání lomítka a číslice pět jak je vidět na obrázku 4.16.



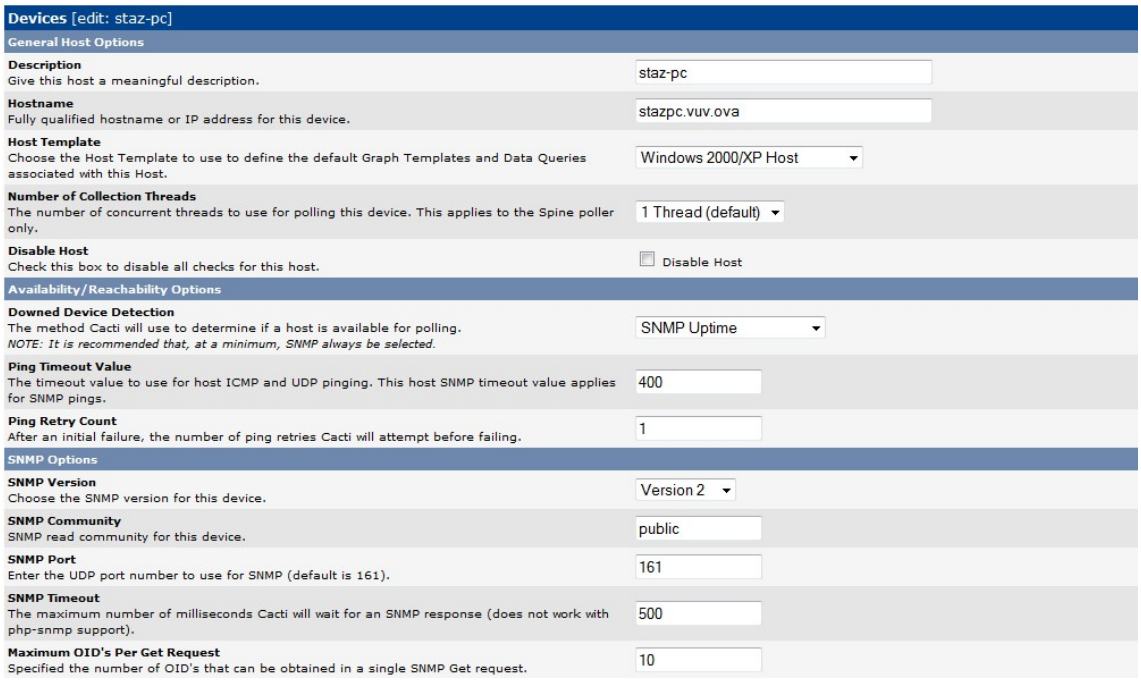
Obrázek 4.15: Původní nastavení spouštění skriptu v deamonu Cron



Obrázek 4.16: Nové nastavení spouštění skriptu v deamonu Cron

Spouštění skriptu se nastavuje na prvních pěti pozicích. První pozice určuje minutu, druhá hodinu, třetí den v měsíci, čtvrtá měsíc a pátá pozice den v týdnu. Hvězdička místo čísla znamená, že se na danou hodnotu nebere ohled. Pět hvězdiček znamená, že se bude daný skript spouštět každou minutu. Hvězdička znamená to samé jako */1.

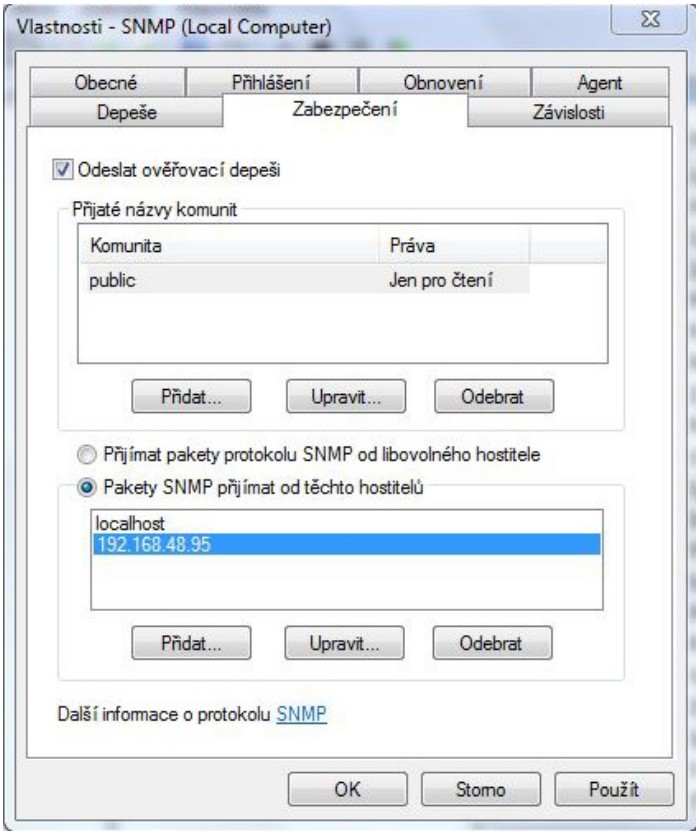
Tímto je systém Cacti nastavený. Přešel jsem zpátky do webového rozhraní a z levého panelu jsem vybral Device pro nastavení zařízení. Vypsal jsem popis (Description), doménové jméno (Hostname). Je možné napsat i IP adresu. A šablonu hosta (Host Template) jsem nastavil Windows 2000/XP Host. Je možné nechat i Generické nastavení. Zkontroloval jsem nastavení verze SNMP. Vzhledem k tomu, že většina zařízení podporuje SNMPv2 nastavil jsem verzi 2. Název komunity jsem nechal public. Ostatní nastavení není potřeba měnit. Obrázek 4.17 znázorňuje nastavení monitorování mého počítače.



Obrázek 4.17: Nastavení zařízení pro monitorování

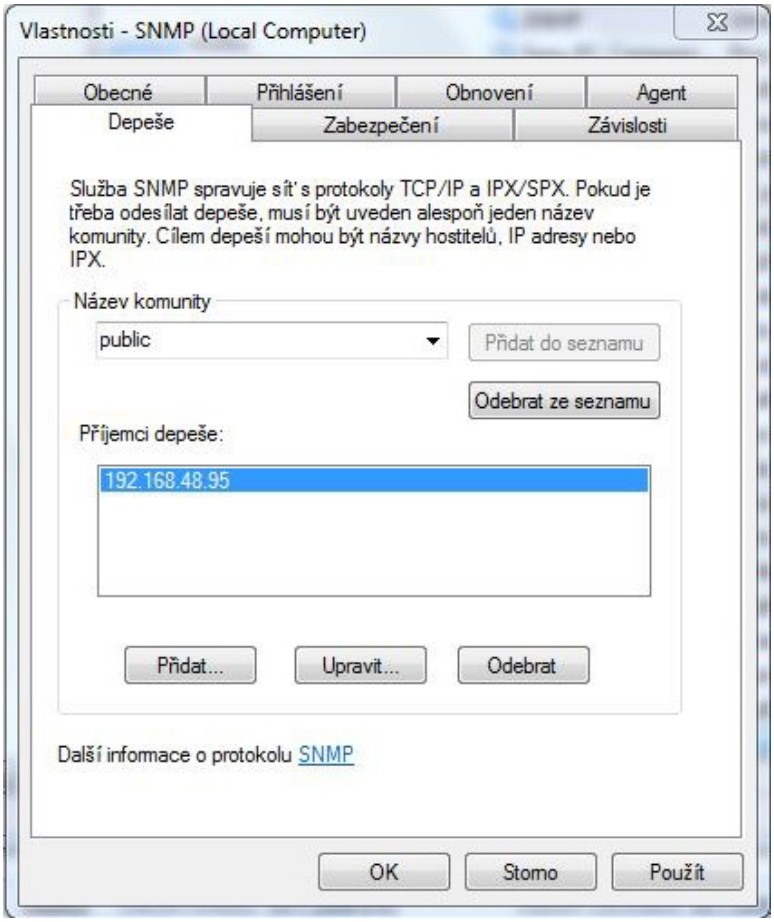
Jakmile jsem vytvořil zařízení (po kliknutí vpravo dole na Create) mohl jsem vytvořit první graf. Vpravo nahoře jsem klikl na Create Graphs for this Host. Z nabízených rozhraní jsem si vybral to, které chci monitorovat a dal sem jsem vytvořit. Aby host, tedy můj počítač, odpovídat na zprávy od systému Cacti, musel jsem jej nastavit. Ve Windows 7 Professional v ovládacích panelech jsem otevřel Programy a funkce. Z levého menu vybeal Zapnout nebo vypnout funkce systému Windows a našel Protokol SNMP, který jsem označil a potvrdil tlačítkem OK.

Vrátil jsem se zpátky do ovládacího panelu, zvolil nástroje pro správu a otevřel Služby. V seznamu jsem našel SNMP a otevřel vlastnosti. Na kartě Zabezpečení jsem nastavil jméno komunity a IP adresu pro příjem SNMP paketů. Nastavení zobrazuje obrázek 4.18.



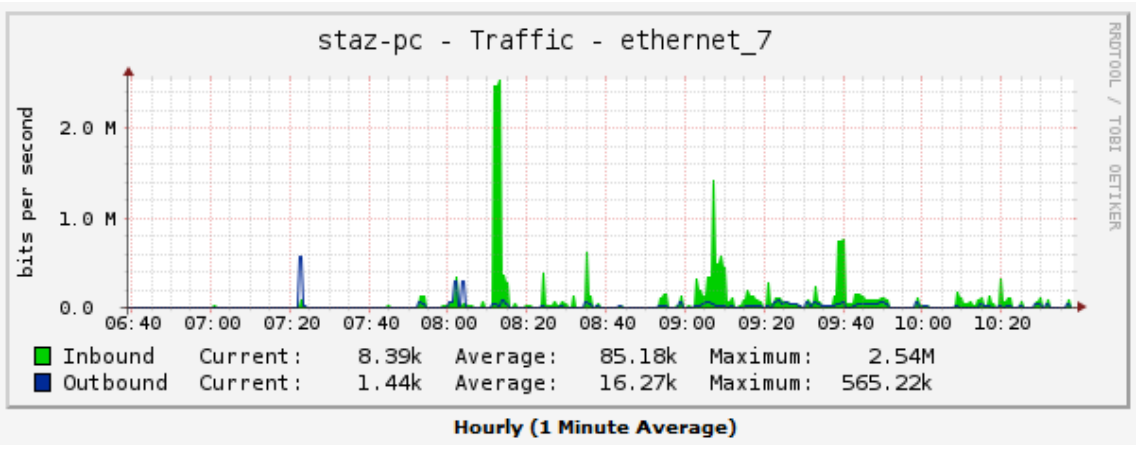
Obrázek 4.18: Nastavení zabezpečení ve vlastnostech SNMP

Nastavil jsem také posílání depeší jak je vidět na obrázku 4.19. Pro funkčnost mého monitoringu to však není toto nastavení důležité. Nastavení je potřeba potvrdit tlačítkem OK. Popis nastavení je také uveden na webových stránkách [29].



Obrázek 4.19: Nastavení odesílání depeší

Graf si můžeme zobrazit v systému Cacti přepnutím záložky vlevo nahoře ve webovém prohlížeči. Za pár hodin se zobrazil graf, jak je vidět na obrázku 4.20. Po kliknutí na graf si můžeme prohlédnout provoz za uplynulé hodiny, dny, měsíce nebo rok.



Obrázek 4.20: Graf přenášených dat z přepínače do PC

5 Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné v průběhu odborné praxe

Při své odborné praxi jsem využil doposud získané teoretické znalosti z předmětu počítačových sítí ze třetího ročníku. Jednalo se o znalosti aktivních zařízení, topologií sítí, různých protokolů a technologií, které slouží pro chod počítačových sítí LAN. Díky těmto znalostem jsem se celkem rychle zorientoval ve firemní síti. Doposud jsem neměl téměř žádné zkušenosti s návrhem počítačové sítě, proto byly znalosti získané v tomto předmětu pro mne odrazovým můstkem. Bez znalostí získaných v předmětu počítačové sítě, bych se při testování firewallu na směrovači MikroTik jen těžko orientoval.

Přínosem pro mě byl i předmět praktikum komunikačních sítí, ve kterém jsem získal základní znalosti operačního systému Ubuntu, které jsem v průběhu praxe mnohokrát využil, především v testovací části mé odborné praxe.

6 Scházející znalosti a dovednosti v průběhu odborné praxe

Na praxi jsem se zaměřoval především na firemní počítačovou síť LAN. I přes absolvování předmětů Počítačové sítě a Praktikum komunikačních sítí mi scházeli znalosti v oblasti Windows serverů a práce s operačním systémem Windows při nastavování služeb. Dále jsem dohánět nedostatky v oblasti protokolu SNMP, který se běžně používá v počítačové sítí LAN.

Doposud jsem neměl téměř žádné zkušenosti s analýzou a návrhem počítačové sítě LAN. Veškeré informace jsem hledal na internetu.

Novinkou pro mě byl směrovač MikroTik, který nabízel velkou škálu možností a nastavení pro počítačové sítě LAN. Jeho využití je poměrně široké a lze jej zařadit mezi kvalitní zařízení pro realizaci počítačové sítě.

7 Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Odborná praxe mi dala spoustu praktických zkušeností s analýzou, návrhem a monitoringem počítačové sítě LAN. Získal jsem povědomí o tom, jak firemní síť funguje, jaké služby může nabízet, a jak je potřeba přistupovat k problémům. Získal jsem návyk na metodické postupy práce, kdy je potřeba předem naplánovat jednotlivé úkony. Dále jsem získal schopnosti orientovat se v počítačové síti, v struktuře kabeláže a v datovém rozvaděči, kdy na první pohled nemusí být zřejmé, o jakou topologii sítě se jedná.

Při hledání informací ohledně analýzy počítačové sítě jsem se dozvěděl spoustu užitečných informací o zabezpečení zařízení, které i když byly nad rámec odborné praxe, byly pro mě přínosné, neboť bych se rád do budoucna zabýval otázkou bezpečnosti počítačových sítí.

Nová počítačová síť je mnohem přehlednější než původní. Díky rozdělení adresního prostoru dle zařízení lze již jednoduše určit dle příchozí IP adresy, o jaké zařízení se jedná. Z vytvořených dokumentů o přepínačích lze jednoduše vyčíst, které zařízení se nachází ve kterém portu daného přepínače a lze tak dohledat například závady nebo odpojit zařízení od sítě bez zdlouhavého hledání zapojení. Monitoring sítě dává správci sítě navíc přehled nad množstvím přenášených dat počítačovou sítí.

Odbornou praxi hodnotím pozitivně a mohu jen doporučit jako formu zpracování bakalářské práce. Myslím si, že praxe v mém oboru je nejen vítaná, ale i požadovaná budoucími zaměstnavateli. Pro mě byla tato praxe přínosná a jsem rád, že mi bylo umožněno ji absolvovat.

Použitá literatura

[1] Angry IP Scanner. [online]. [cit. 2014-10-09]. Dostupné z: http://angryip.org/

[2] Advanced IP Scanner. [online]. [cit. 2014-10-09]. Dostupné z: http://www.advanced-ip-scanner.com

[3] Zenmap – Official cross-platform Nmap Security Scanner GUI. [online]. [cit. 2014-10-10]. Dostupné z: https://nmap.org/zenmap/

[4] UTM & Next-Gen Firewall . [online]. [cit. 2014-10-31]. Dostupné z: https://www.sophos.com/en-us/products/unified-threat-management.aspx

[5] Documentation – Sophos Technical Support. [online]. [cit. 2014-10-31]. Dostupné z: https://www.sophos.com/en-us/support/documentation.aspx

[6] ZyXEL. Datasheet GS2200. [online]. [cit. 2014-11-6]. Dostupné z: ftp://ftp.zyxel.com/GS2200-24/datasheet/GS2200-24_4.pdf

[7] ZyXEL. [online]. [cit. 2014-11-06]. Dostupné z: ftp://ftp.zyxel.com/GS2200-24/

[8] 3Com Baseline Switch 2924-SFP. cnet. [online]. [cit. 2014-11-06]. Dostupné z: http://www.cnet.com/products/3com-baseline-switch-2924-sfp-plus-switch-24-ports-managed-desktop-series/specs/

[9] NETGEAR Support | GS724TP | Advanced Smart Switches. [online]. [cit. 2014-11-06]. Dostupné z: http://support.netgear.com/product/GS724TP

[10] TL-SG2216WEB. TP-LINK. [online]. [cit. 2014-11-06]. Dostupné z: http://www.tp-link.com/en/products/details/cat-0_TL-SG2216WEB.html

[11] 3Com Baseline Switches. MAXDATA. [online]. [cit. 2014-11-06]. Dostupné z: http://ftp.maxdata.de/Accessories/Connectivity/3Com/Datasheets/200800_3Com_Baseline_2016.pdf

[12] Petr Bouška. Cisco IOS 9 – Spanning Tree Protocol. SAMURAJ-cz.com. [online]. 20.08.2007 [cit. 2015-01-09]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-9-spanning-tree-protocol/

[13] Petr Bouška. VLAN – Virtual Local Area Network. SAMURAJ-cz.com. [online]. 02.06.2007 [cit. 2015-01-09]. Dostupné z: http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

[14] Petr Bouška. SNMP – Simple Network Management Protocol. SAMURAJ-cz.com. [online]. 20.12.2006 [cit. 2015-01-09]. Dostupné z: http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/

[15] Net-SNMP. [online]. [cit. 2015-01-09]. Dostupné z: http://www.net-snmp.org/

[16] Bráníme se odposlechu: obrana na switchi. Lupa.cz. [online]. 22.8.2006 [cit. 2015-01-15]. Dostupné z: http://www.lupa.cz/clanky/branime-se-odposlechu-obrana-na-switchi/

[17] Petr Bouška. Cisco IOS 13 – DHCP služby na switchi. SAMURAJ-cz.com. [online]. 06.01.2008 [cit. 2015-01-15]. Dostupné z: http://www.samuraj-cz.com/clanek/cisco-ios-13-dhcp-sluzby-na-switchi/

[18] Petr Bouška. Běžné útoky na switche, Cisco Dynamic ARP Inspection. SAMURAJ-cz.com. [online]. 18.06.2009 [cit. 2015-01-15]. Dostupné z: http://www.samuraj-cz.com/clanek/bezne-utoky-na-switche-cisco-dynamic-arp-inspection/

[19] Petr Bouška. Připojení rychlejší a spolehlivější. SAMURAJ-cz.com. [online]. 15.11.2009 [cit. 2015-01-15]. Dostupné z: http://www.samuraj-cz.com/clanek/pripojeni-rychlejsi-a-spolehlivejsi/

[20] Routerboard RB750GL. Routerboard.com. [online]. [cit. 2014-12-11]. Dostupné z: http://routerboard.com/RB750GL

[21] MikroTik Routers and Wireless. [online]. [cit. 2014-12-11]. Dostupné z: http://www.mikrotik.com/

[22] Classless Inter-Domain Routing. Wikipedia.org. [online]. [cit. 2015-01-23]. Dostupné z: http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

[23] Petr Bouška. Začínáme s monitoringem sítě. SAMURAJ-cz.com. [online]. 01.09.2009 [cit. 2015-02-19]. Dostupné z: http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/

[24] Cacti. [online]. [cit. 2015-02-25]. Dostupné z: http://cacti.net/

[25] ZABBIX. [online]. [cit. 2015-02-25]. Dostupné z: http://www.zabbix.com/

[26] Nagios. [online]. [cit. 2015-02-25]. Dostupné z: http://www.nagios.org/

[27] RRDTool. oetiker.ch. [online]. [cit. 2015-02-19]. Dostupné z: https://oss.oetiker.ch/rrdtool/

[28] CronHowto – Community Help Wiki. ubuntu.com. [online]. [cit. 2015-02-27]. Dostupné z: https://help.ubuntu.com/community/CronHowto

[29] Applications Manager – SNMP Agent Configuration,Monitoring SNMP Resources,SNMP Agent Management. manageengine.com. [online]. [cit. 2015-03-05]. Dostupné z: https://www.manageengine.com/products/applications_manager/help/appendix/snmp-agent-configuration.html